Wisconsin ServicePoint

RIGHT TO DENY USER OR PARTNERS ACCESS

Policy:
A participating Agency or a user's access may be suspended or revoked for suspected or actual violation of the security protocols.

Standard:
Serious or repeated violation by users of the system may result in the suspension or revocation of an agency's access.

Purpose:
To outline consequences for failing to adhere to information security protocols.

Resources:

HMIS WEB SITE (WISP)
https://wisconsin.servicept.com

HMIS INFOrmed
www.hmis.info/default.asp

Wisconsin HMIS
http://wisp.wi.gov

WISP HELP
sphelp@commerce.state.wi.us

Violations of security procedures will be sanctioned.

All potential violations of any security protocols will be investigated.

If possible, all confirmed violations will be communicated in writing to the affected client within 14 days, unless the client cannot be located. If the client cannot be located, a written description of the violation and efforts to locate the client will be prepared by the Commerce HMIS staff and placed on file in a client file at the Agency that originated the client's record..

Any user found to be in violation of security protocols will be sanctioned accordingly.

Sanctions may include but are not limited to; a formal letter of reprimand, suspension of system privileges, revocation of system privileges and criminal prosecution.

Any agency that is found to have consistently and/or flagrantly violated security protocols may have their access privileges suspended or revoked.

All sanctions are imposed by the Department of Commerce HMIS staff.

All sanctions can be appealed to the HMIS Steering Committee.